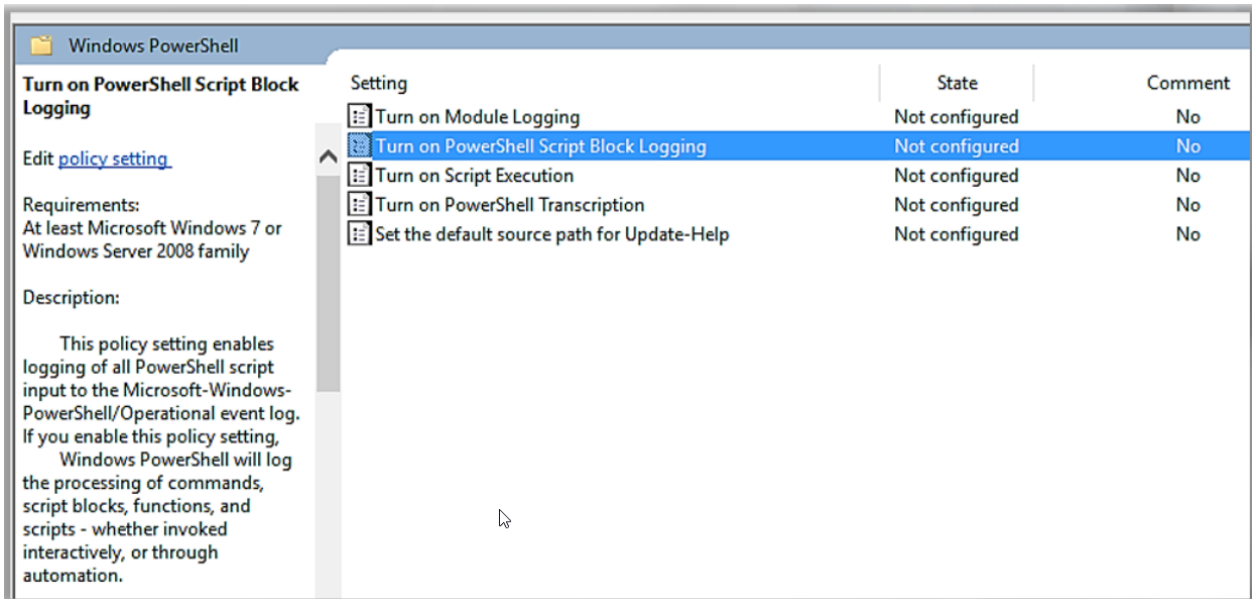
Unmanaged PowerShell:

PowerShell was created for admins but it turned into a big risk. Attackers use PowerShell not only to avoid detection by injecting code in memory but also bypass restriction and white-listing as its already part of the OS.

In response to that MS released better logging capability for PowerShell and now if we see Malicious PowerShell scripts, we can submit it to AMSI which is Antimalware interface.

PowerShell logging is great when we are hunting for malicious commands, and the scripts, this way we can see the PowerShell script that run as its going to be logged.

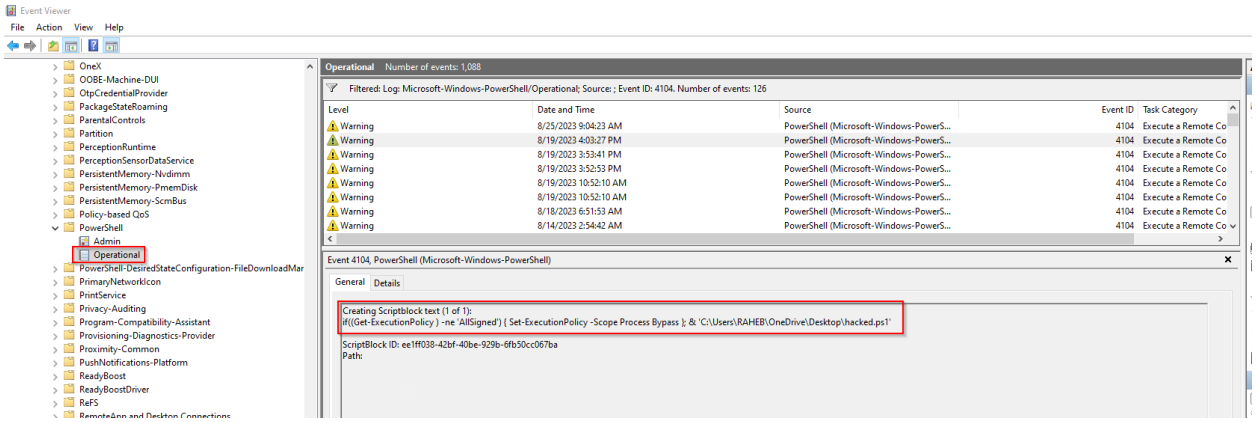
We have to enable this Logging feature and its called “PowerShell Script Block Logging”. To enable it we go to the Group policy and then “Services logs > Microsoft > Windows > PowerShell/operational ”



Here we can enable the 1st one, the 2nd one and the 4th one.

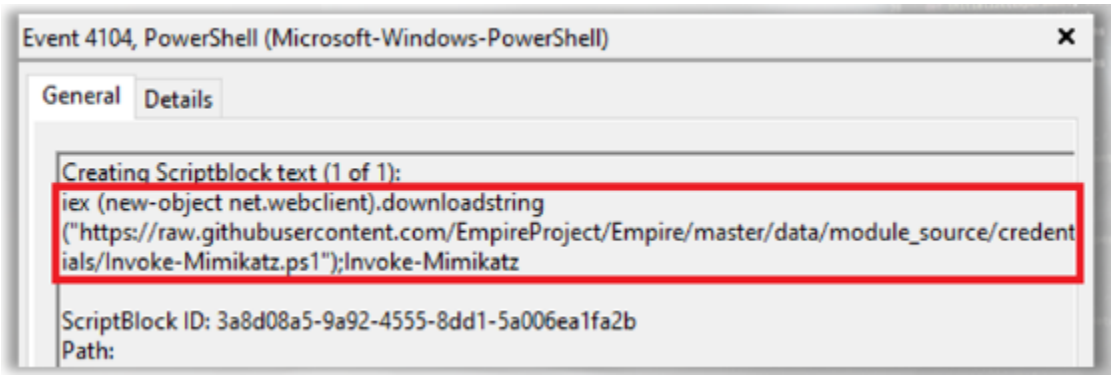
And to hunt for PowerShell we will look or hunt for Event ID 4104,4105 and 4106.

Here is an example of event ID 4104:



Here we see the script file that run:

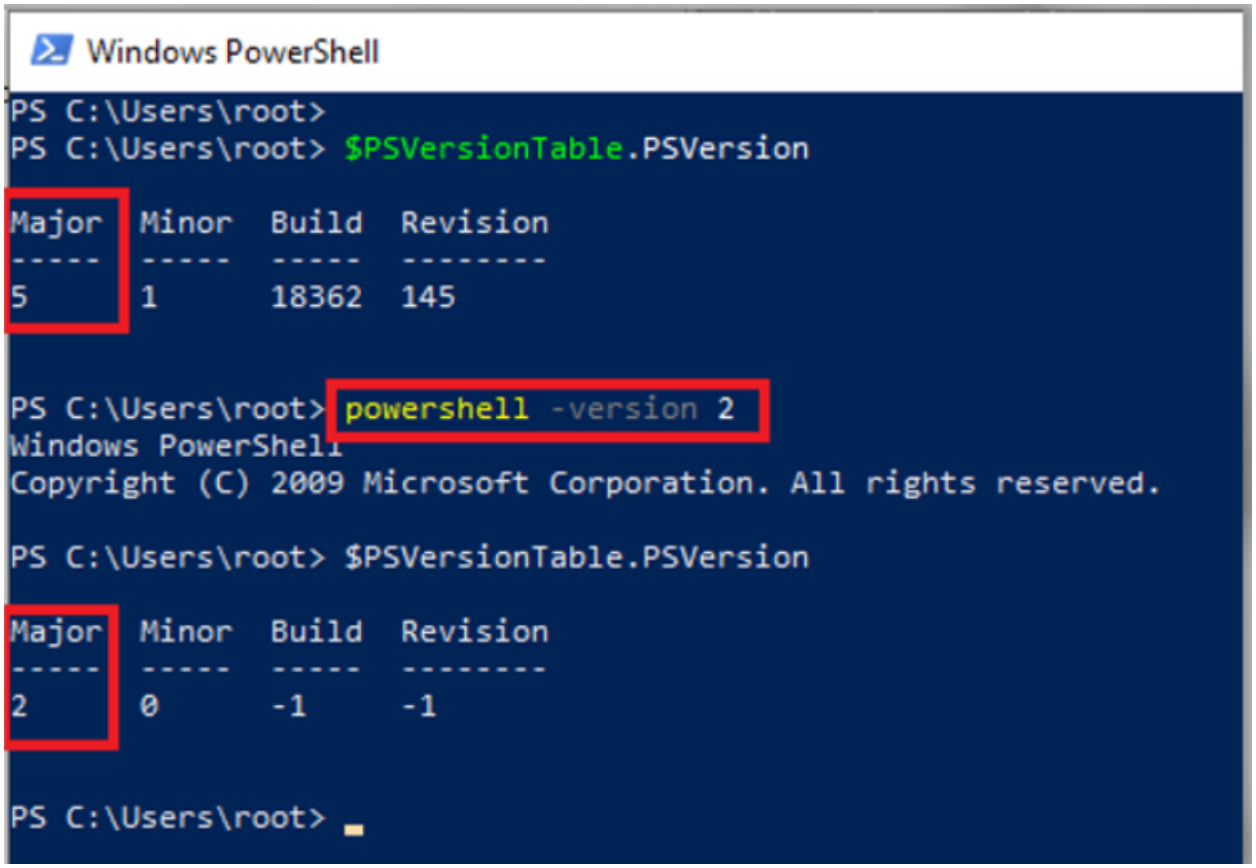
Another example of 4104, where the mimikatz.ps1 script is run



Here we see the net.webclient which means it download something using powershell, mean this is the script or command that download something from the internet which is downloading the mimikatz.ps1 which is tool that dump the credentials.

As we know the PowerShell logging was added in Version 5 of the PowerShell but attackers may downgrade the PowerShell version to like version 2 as it will not have the Logging capability, or they attacker will try to disable the logging on the host.

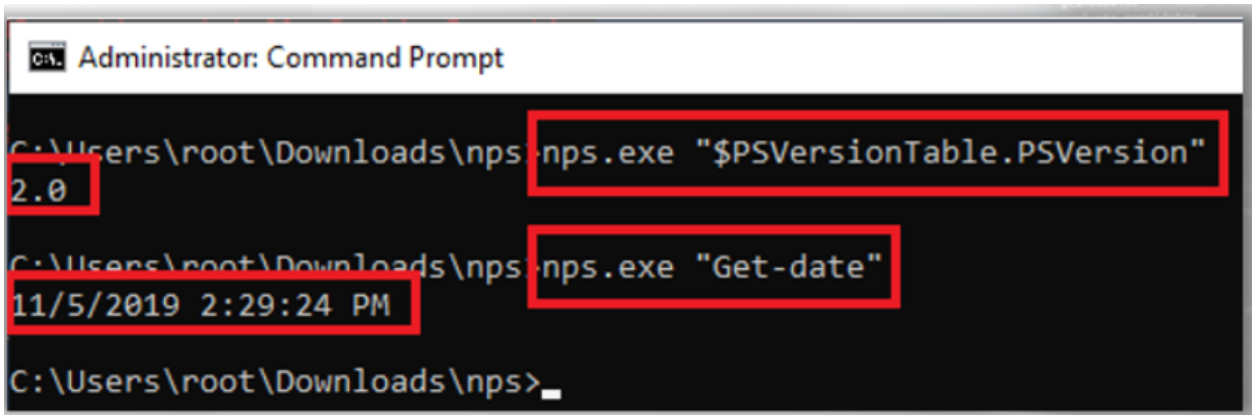
Downgrading PowerShell:



there is obfuscation techniques such as “invoke-obfuscation” project, it become difficult to detect malicious command line arguments.

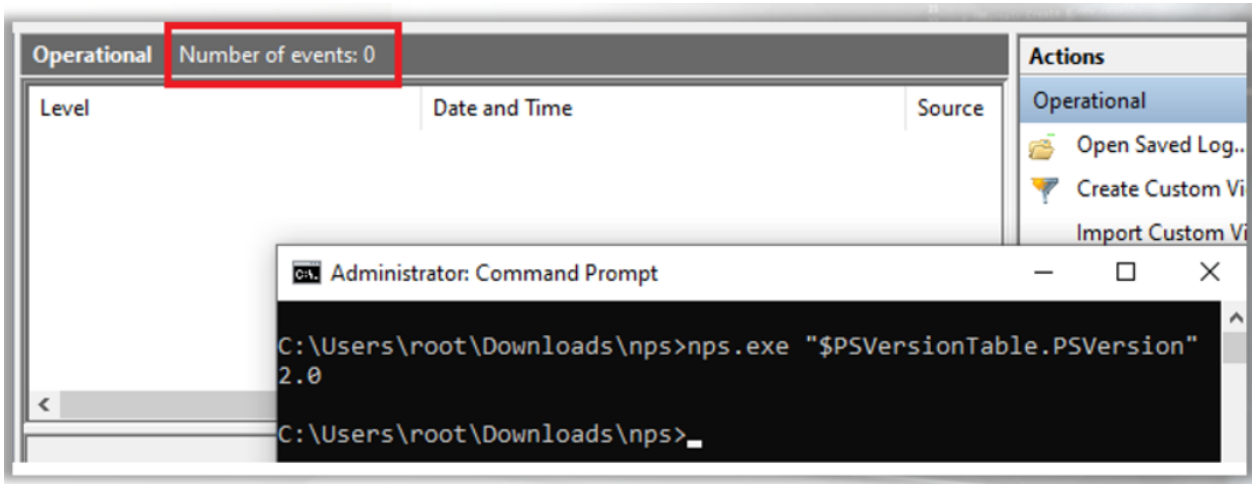
PowerShell is not limited to “powershell.exe”, mean it’s a wrapper for “System.Managment.Automation.dll” so other application can run PowerShell code too.

Someone made a project called NPS (Not PowerShell Project). With NPS binary we can run any PowerShell command and event we can run PowerShell command under old version like version 2.



Details and Download link is: https://github.com/Ben0xA/nps

As we said before that the Version 2 of powershell dosnt have the Logging capability:



Hunting for Unmanaged Powershell:

- Usage of “System.managment.Automation.dll” process that is not “powershell.exe” or “powershell_ise.exe”, mean if we see it, then other program is running the powershell commands like the way NPS do it.
- Event IDs 400 and 800, where the Engine version is lower that the PowerShell version, mean someone downgraded the version. Like this: